IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
(Attorney Docket No. 14822US02)

In the Application of:

Jeyhan Karaoguz, et al.

Serial No. 10/675,491

Filed: September 30, 2003

For: Method and System for Secure Linking with Authentication and Authorization in a Media Exchange Network

Examiner: Ryan, Patrick A.

Group Art Unit: 2427

Confirmation No. 6014

Electronically Filed on May 27, 2009

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Applicants respectfully request that the Board of Patent Appeals and Interferences reverse the final rejection of claims 1-26 of the present application. This Appeal Brief is timely because it is being concurrently filed with a Notice of Appeal within 3 months of the March 9, 2009 mailing date of the Final Office Action.

REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

The real party in interest is Broadcom Corporation, having a place of business at 16215 Alton Parkway, Irvine, California.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

Not applicable.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

The present application includes claims 1-26, all of which stand rejected.[1] The Applicants identify claims 1-26 as the claims that are being appealed. The text of the claims involved in this Appeal, namely, claims 1-26, is provided in the Claims Appendix.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

Claims 1-26 were finally rejected.[2] None of these claims were amended after being finally rejected. Instead, the Applicants submit a Notice of Appeal and this Appeal Brief in response to the Final Office Action.

---

[1] *See* March 9, 2009 Final Office Action.
[2] *See id.*

SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

Independent claim 1 recites the following:

A method for establishing a communication pathway for subsequent media exchanges between a television display[3] in a first home[4] and storage[5] that contains media in a second[6] home,[7] the method comprising:

securely receiving address correlation information associated with the television display in the first home;[8]

securely receiving address correlation information associated with the storage in the second home;[9]

requesting affirmative confirmation[10] using said received address correlation information associated with one or both of the television display and/or the storage;[11] and

storing said affirmative confirmation.[12]

Dependent claim 2 recites the following:

The method according to claim 1, comprising associated with the subsequent

---

[3] *See id., e.g.,* at page 13, line 27 to page 14, line 1, page 25, lines 4-5, Figure 6, ref. 608.
[4] *See id., e.g.,* at page 10, lines 19-21, Figure 1, ref. 104, Figure 3, ref. 303, Figure 4, ref. 403.
[5] *See id., e.g.,* at page 13, lines 21-26.
[6] *See id., e.g.,* at page 10, lines 21-23, Figure 1, ref. 108, Figure 3, ref. 310, Figure 4, refs. 409, 412.
[7] *See* present application, *e.g.,* at page 4, lines 2-4, page 9, lines 2-4.
[8] *See id., e.g.,* at page 4, lines 4-6, page 9, lines 4-6, page 14, lines 17-19, Figure 2A, ref. 201.
[9] *See id., e.g.,* at page 4, lines 6-7, page 9, lines 6-7, page 14, lines 21-27.
[10] *See id., e.g.,* at page 15, lines 1-8, page 16, lines 13-20, page 18, lines 16-24.
[11] *See id., e.g.,* at page 4, lines 7-9, page 9, lines 7-9.
[12] *See id., e.g.,* at page 4, lines 7-9, page 9, lines 7-9.

media exchanges, verifying that said affirmative confirmation has been stored.[13]

Independent claim 6 recites the following:

A method for establishing a communication pathway for subsequent media exchange between a first media component in a first home and a second media component in a second home,[14] the method comprising:

receiving at least one of address correlation information associated with the first media component in the first home and a routing address associated with the first media component in the first home;[15]

receiving address correlation information associated with the second media component in the second home;[16] and

requesting confirmation[17] using the address correlation information associated with the second media component.[18]

Dependent claim 7 recites the following:

The method according to claim 6, comprising storing said confirmation.[19]

Dependent claim 8 recites the following:

The method according to claim 7, comprising associated with the subsequent media exchange, verifying that said confirmation has been stored.[20]

Independent claim 12 recites the following:

A system that supports media exchange between a first home and a second home,[21] the system comprising:

---

[13] *See id., e.g.,* at page 4, lines 10-11, page 5, lines 2-3, page 9, lines 9-11 and 20-22.
[14] *See id., e.g.,* at page 4, lines 22-24, page 9, lines 12-15.
[15] *See id., e.g.,* at page 4, lines 25-27, page 9, lines 15-17.
[16] *See id., e.g.,* at page 4, lines 27-28, page 9, lines 17-19.
[17] *See id., e.g.,* at page 15, lines 1-8, page 16, lines 13-20, page 18, lines 16-24
[18] *See id., e.g.,* at page 5, lines 1-2, page 9, lines 19-20.
[19] *See id., e.g.,* at page 4, lines 7-9, page 9, lines 7-9.
[20] *See id., e.g.,* at page 4, lines 10-11, page 5, lines 2-3, page 9, lines 9-11 and 20-22.
[21] *See id., e.g.,* at page 5, lines 11-12, page 34, lines 10-11.

a television display in the first home, said television display having an associated first routing address;[22]

storage that contains media in a second home,[23] said storage having an associated second routing address;[24] and

a server component that establishes a secure communication pathway through which media contained in the second home is delivered to said television display in the first home,[25] wherein one or more of said television display, said storage and/or said server requests affirmative confirmation[26] using one or both of said first and/or second associated routing addresses.[27]

Independent claim 16 recites the following:

A system for communicating information,[28] the system comprising:

at least one processor that issues access information from a first device to at least a second device;[29]

said at least one processor transfers at least a portion of said access information to a third device;[30] and

said at least one processor authenticates said access information by said first device when said third device attempts to transfer at least one of media data and service to said at least said second device.[31]

---

[22] *See id., e.g.,* at page 5, lines 12-13, page 34, lines 11-12.
[23] *See id., e.g.,* at page 5, lines 13-14, page 34, lines 11-13.
[24] *See id., e.g.,* at page 5, lines 14-15, page 34, lines 13-14.
[25] *See id., e.g.,* at page 5, lines 15-17, page 34, lines 14-16.
[26] *See id., e.g.,* at page 15, lines 1-8, page 16, lines 13-20, page 18, lines 16-24
[27] *See id., e.g.,* at page 5, lines 1-2, page 15, lines 1-8, page 16, lines 13-20, page 18, lines 16-24..
[28] *See id., e.g.,* at page 5, lines 24-25, page 9, lines 23-25.
[29] *See id., e.g.,* at page 5, lines 26-27, page 9, lines 25-26, page 32, lines 14-18, page 34, lines 24-26.
[30] *See id., e.g.,* at page 5, lines 28-29, page 9, lines 26-27, page 32, lines 18-19, page 34, lines 26-28..
[31] *See id., e.g.,* at page 5, line 29 to page 6, line 3, page 9, line 27 to page 10, line 10, page 32, lines 29-20, page 34, line 27 to page 35, line 1.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

- Claims 1-12, 14 and 15 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. 6,774,926 ("Ellis") in view of U.S. 2003/0177249 ("Takanashi").
- Claim 13 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis in view of Takanashi and U.S. 6,182,094 ("Humpleman").
- Claims 16-18 and 20-26 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis in view of U.S. 2002/0004832 ("Yoon").
- Claim 19 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis in view of Yoon and U.S. 6,934,858 ("Woodhill").

ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

I. The Proposed Combination Of Ellis And Takanashi Does Not Render Claims 1-12 And 14-15 Unpatentable

The Applicants first turn to the rejection of claims 1-12, 14 and 15 as being unpatentable over Ellis in view of Takanashi. "To establish *prima facie* obviousness of a claimed invention, **all** the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)." *See* Manual of Patent Examining Procedure (MPEP) at 2143.03 (emphasis added). Further, "'**[a]ll words** in a claim must be considered in judging the patentability of that claim against the prior art.' *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA)." *See id.*

Claim 1 recites the following:

> A method for establishing a communication pathway for subsequent media exchanges between a television display

> in a first home and storage that contains media in a second home, the method comprising:
>
> securely receiving address correlation information associated with the television display in the first home;
>
> securely receiving address correlation information associated with the storage in the second home;
>
> requesting affirmative confirmation using said received address correlation information associated with one or both of the television display and/or the storage; and
>
> storing said affirmative confirmation.

A. The Proposed Combination Of References Does Not Describe, Teach Or Suggest "Requesting Affirmative Confirmation Using Said Received Address Correlation Information Associated With One Or Both Of The Television Display And/Or The Storage"

The Office Action acknowledges that "Ellis does not teach securely transferring said addressing information between a television in a first home and a storage in a second home or requesting confirmation of the security information." *See* March 9, 2009 at page 8. Indeed, the Office Action seemingly relies on Ellis as disclosing only the preamble of claim 1. *See id.* at pages 8-9.

In an attempt to overcome these deficiencies, the Office Action relies on Takanashi. *See id.* Takanashi "relates generally to dynamic IP address assignment, and more particularly, but not exclusively, provides a system and method for limiting unauthorized access to a network by assigning a random DHCP [Dynamic Host Configuration Protocol] renewal time window to a wireless client." *See* Takanashi at [0002]. Takanashi discloses a system that performs the following process:

> receiving a request for an IP address from a wired or wireless agent; determining an IP address to assign; randomly determining a leasing time and/or renewal window; and transmitting the IP address, leasing time, and renewal window to the client in a DHCP reply packet. The method further comprises ... receiving the DHCP reply packet;

> starting a timer; listening for a renewal packet during the renewal window; and terminating access to a network if no renewal packet is received during the renewal window.

See id. at [0009] and [0034]-[0036]. Thus, Takanashi discloses a system and method that begins with a request for an IP address. The IP assignment system then determines an IP address to assign and randomly determines a leasing time and/or renewal window. This information is then transmitted to a client in a DHCP reply packet. The access system then receives the DHCP reply packet, starts a timer and listens for a renewal packet. If no renewal packet is received during a renewal window, access to the network is terminated. "If a renewal packet is received during the renewal window, then the starting, listening and subsequent steps are repeated." *See id.* at [0009].

In Takanashi, the "IP assignment engine 300 listens for a **request <u>for an IP address</u>** and assigns an IP address to the requesting client." *See id.* at [0028] (emphasis added). A request for an IP address is not, however, a request for confirmation, in general, nor a request for confirmation using received address correlation information associated with one or both of a television display and/or a storage, in particular. That is, an IP address request may be made without requesting confirmation, and clearly without requesting confirmation using received address correlation information associated with one or both of a television and/or a storage. Takanashi does not describe, teach or suggest such a request for confirmation, generally, or one as specifically recited in claim 1, for example. Instead, the request disclosed in Takanashi is merely one for an IP address.

Takanashi also discloses that the "[a]ccess engine 420 enables a client to access network 110 upon assignment of an IP address and validation of a user ID and password received from the client." *See id.* at [0031]. The "access engine 420 validates the user ID and password by cross checking user ID and password data in database 130." *See id.* That is, a user enters a user ID and password, which are then validated by those stored in a database. However, entering a user ID and password is

not a request for anything, let alone a request for "requesting affirmative confirmation using said received address correlation information associated with one or both of the television display and/or the storage," as recited in claim 1, for example. Thus, for at least this reason, the proposed combination of Ellis and Takanashi does not render claim 1 or the claims that depend therefrom unpatentable.

The Office Action states, however, the following:

> The Examiner has addressed the act of "requesting affirmative confirmation" with Takanashi's teachings of a client device logging onto Network 110, which requires a valid IP address, and a User ID and password (Office Action Page 5; Takanashi [0022-0024]). It is the Examiner's position that the client device is requesting a confirmation of the data provided (i.e. IP address, User ID, password) by way of the login process, where this data is "judged valid per data in user database 130" (as Takanashi discloses in Paragraph [0023]) and when this data is found to be valid, the client device is provided access to Network 110.

See March 9, 2009 Office Action at pages 3-4. This subjective notion of a request for affirmative confirmation simply does not harmonize with the plain meaning of the relevant limitations of claim 1. The Office Action does not clearly indicate what it considers the "request" (e.g., does it consider merely "logging in" a request? A password? A user ID?) or the "affirmative confirmation" (the Office Action simply does not explicitly point out what it considers the affirmative confirmation that is being requested)

The mere act of "logging onto" a network using an IP address, a user ID and/or password is by no means a "request." Instead, it is merely an action of logging onto the network. Moreover, the Office Action asserts that **Ellis** discloses a viewer entering "a password" (*see id.* at page 7) but acknowledges that "Ellis does not teach securely transferring authorization and addressing information between a television in a first home and a storage in a second home or **requesting confirmation of the securing information**." *See id.* at page 8. Therefore, the Office Action seemingly acknowledges

that the mere act of logging on using a password is not a request, in general, or a request for affirmative confirmation, in particular.

Further, even if one assumes that logging onto a network was a "request" (the Office Action being unclear as to whether it makes this assumption, but the Applicants clearly do not make such an assumption), it still is not a **request for affirmative confirmation**. While the Office Action summarily concludes that logging onto a network using an IP address, a user ID and password is a "request for affirmative confirmation," the Office Action simply does not explain where the request is found in this process of logging onto the network, nor where there is any specific **request for affirmative confirmation**. For at least the reasons discussed above, the Applicants respectfully request reconsideration of the claim rejections.

Claim 6 recites, in part, "requesting confirmation using the address correlation information associated with the second media component." Claim 12 recites, in part, "said **server requests affirmative confirmation using one or both of said first and/or second associated routing addresses**." For at least the reasons discussed above with respect to claim 1, the Applicants respectfully submit that the proposed combination of Ellis and Takanashi does not render claims 6, 12 or those that depend therefrom unpatentable. .

B. The Proposed Combination Of References Does Not Describe, Teach Or Suggest Storing A Request For Confirmation, As Recited In Claims 1 And 7

The proposed combination of Ellis and Takanashi does not render claim 1 unpatentable for an additional reason. While Takanashi discloses that user ID and password information are stored in a database (*see* Takanashi at [0031]), these are, again, just a user ID and password, but not a request, and certainly not a request for confirmation. That is, stored user ID and password information are not the same as a stored affirmative confirmation.

The Office Action has not cited anything that describes, teaches or suggests "**storing said affirmative confirmation**," as recited in claim 1. Indeed, the Office

Action merely states "IP Assignment System 125 forwards the IP address, leasing time, and renewal window data to the client in a DHCP replay packet ("Storing Affirmative Confirmation"), **as Takanashi discloses in Paragraph [0022]**." *See* March 9, 2009 Office Action at page 8 (emphasis added). As shown, the Office Action conveniently attaches "Storing Affirmative Confirmation" to reasoning that does not relate to such a statement. Further, the Office Action relies on Takanashi at [0022] as disclosing "storing affirmative confirmation."

Takanashi discloses, however, the following:

> IP assignment system 125 receives a DHCP broadcast from a client (wired or wireless) requesting an IP address. In response, system 125 assigns an IP address and randomly assigns a leasing time and/or renewal window (including random window length and/or random start window start time with a fixed interval). The system 125 then forwards the IP address, leasing time, and renewal window data to the client in a DHCP reply packet. IP assignment system 125 will be discussed in further detail in conjunction with FIG. 3 and FIG. 6 below.

See Takanashi at [0022]. Again, this portion of Takanashi discloses a request, but that request is only for an IP address. There simply is nothing in this portion, nor in the remainder, of Takanashi that describes, teaches or suggests a request for confirmation. Additionally, there simply is nothing in that describes, teaches or suggests any storage of confirmation.

Thus, for at least these additional reasons, the proposed combination of Ellis and Takanashi does not render claim 1 or the claims that depend therefrom unpatentable.

Claim 7 recites, in part, "storing said confirmation." As explained above, the proposed combination of Ellis and Takanashi does not describe, teach or suggest storing confirmation. For at least this additional reason, the proposed combination of references does not render claim 7 unpatentable.

II. The Proposed Combination Of Ellis And Takanashi Does Not Render Claims 2 And 8 Unpatentable For An Additional Reason

Claim 2 recites, in part, "associated with the subsequent media exchanges, **verifying that said affirmative confirmation has been stored**." As discussed above, the proposed combination of Ellis and Takanashi does not describe, teach or suggest "storing affirmative confirmation," therefore, it cannot describe, teach or suggest "verifying that said affirmative confirmation has been stored."

Moreover, the Office Action cites Takanashi at [0022], [0023] and [0034]-[0037] as disclosing this limitation. *See* March 9, 2009 Office Action at page 9. However, there is nothing in these cited portions of Takanashi that describes, teaches or suggests storing affirmative confirmation, much less verifying such storage of affirmative confirmation. The Office Action is not clear as to what it specifically regards as a "request," "affirmative confirmation," how such confirmation is stored, and how such storage is verified. Thus, for at least these reasons, the Office Action has not established a *prima facie* case of obviousness with respect to claims 1 or 2. The proposed combination of references simply does not describe, teach or suggest "verifying that said affirmative confirmation has been stored," as recited in claim 2.

Dependent claim 8 recites, in part, "associated with the subsequent media exchange, verifying that said confirmation has been stored." As explained above, the proposed combination of references does not describe, teach or suggest this limitation. Thus, for at least this additional reason, the proposed combination of references does not render claim 8 unpatentable.

III. The Proposed Combination Of Ellis, Takanashi And Humpleman Does Not Render Claim 13 Unpatentable

The Applicants also respectfully request reconsideration of the rejection of claim 13 as being unpatentable over the proposed combination of Ellis in view of Takanashi and Humpleman for at least the reasons discussed above with respect to claims 1 and 12.

IV. The Proposed Combination Of Ellis And Yoon Does Not Render Claims 16-18 And 20-26 Unpatentable

The Office Action acknowledges that "Ellis does not teach a processor used to issue access information to a second and third device by way of a first device or that the processor authenticates access information between the second and third devices." *See* March 9, 2009 Office Action at page 17.

In order to overcome these deficiencies, the Office Action states the following:

> Yoon teaches a **processor, Connection Authentication Server 50**, which communicates access information between the Local Computer 30 and the Internet Server 60, as described in Paragraphs [0030-0032]. **The Connection Authentication Server 50** transfers access information to the **Local Computer 30** through the process of Steps 100 and 102 ["**from first to third device**" where the process resides at the first device]. In addition, the **Connection Authentication Server 50** issues this access information **to the Internet Server 60** is Step 104 of Fig. 4 ["**first to second device**"]. Yoon also teaches that the Local Computer 30 requests connection authentication in Step 100 before requesting the services of Internet Server 60 ["authenticates the access information"] (as described in Paragraphs [0038]-0039], with reference to Fig. 4, with further reference to Step 314 of Fig. 6, as described in Paragraph[s] [0060-0061]).

See id. at pages 17-18 (emphasis added). Thus, the Office Action cites the Connection Authentication Server 50 as the "processor" **and** the "first device," the Internet Server 60 as the "second device" and the local computer 30 as the "third device." *See also id.* at page 4 ("the Examiner has identified Local Computer 30 as the claimed 'third device' and Target Internet Server 60 as the claimed 'second device'"). If one applies this reasoning to the claim language, claim 16 would read as follows:

> at least one **processor [Connection Authentication Server 50]** that issues access information from a **first device [Connection Authentication Server 50]** to at least **a second device [Internet Server 60]**;

> said at least one **processor [Connection Authentication Server 50]** transfers at least a portion of said access information to **a third device [Local Computer 30]**; and
>
> said at least one **processor [Connection Authentication Server 50]** authenticates said access information by said **first device [Connection Authentication Server 50]** when said **third device [Local Computer 30]** attempts to transfer at least one of media data and service to **said at least said second device [Internet Server 60]**.

Further, as noted above, the Office Action cites Yoon at Steps 100 and 314 as disclosing the authentication step.

As an initial matter, the reasoning in the Office Action assumes the Connection Authentication Server is **both** the processor and the first device. Accordingly, the Authentication Server 50 would seemingly have to issue and authenticate access information from itself to itself. However, such a reading is nonsensical, particularly in view of the fact that the claim is written to explicitly indicate that the at least one processor is different than the first device. That is, the Applicants did not draft the claim so that two different terms represented the same device, as such a reading would be confusing. Thus, for at least this reason, the Applicants respectfully submit that the reasoning in the Office Action with respect to claim 16 is flawed and should therefore be reconsidered.

Additionally, claim 16 recites, in part, that the processor "authenticates said access information by said first device," which the Office Action notes is the Connection Server 50, "**when said third device**," which the Office Action notes is the Local Computer 30, "**attempts to transfer at least one of media data and service to said at least said second device**," which the Office Action notes is the Internet Server 60.

Yoon at Step 100 states, however the following:

> **Before requesting services to the target internet server 60**, the local computer 30 requests a connection

> authentication to the connection authentication [sic] server 50 in step 100.

See Yoon at [0038] (emphasis added). Notably, this portion of Yoon states that the local computer 30 requests a connection authentication to the connection authentication server 50 ***before*** **requesting services to the target internet server 60**. It does not indicate, however, that the connection **authentication server 50** authenticates access information by the connection server (as the Office Action necessarily reads the claim based on the statement reproduced above) **when** the **local computer 30 attempts** to transfer at least one of media data and service to the **Internet Server 60**.

Further, with respect to step 314, Yoon states that the following:

> The connection authentication server 50 stores the temporary ID and password "P" in its database and transmits such data to the local computer 30 and the target server 60. Also, all the parameters used for generating the temporary ID and password are transmitted to the target internet server 60.

See id. at [0061]. This portion of Yoon discloses that the connection server 50 stores a temporary ID and password and transmits that information to the local computer and target server 60. However, much like step 100 of Yoon, this portion also does not describe, teach or suggest that the **connection authentication server 50** authenticates access information by the connection server (as the Office Action necessarily reads the claim based on the statement reproduced above) **when** the **local computer 30 attempts** to transfer at least one of media data and service to the **Internet Server 60**. Thus, for at least these reasons, the Applicants respectfully request reconsideration of the rejection of claims 16-18 and 20-26. Indeed, for at least these reasons, the Applicants respectfully submit that a *prima facie* case of obviousness has not been established with respect to these claims.

V. The Proposed Combination Of Ellis, Yoon And Woodhill Does Not Render Claim 19 Unpatentable

The Applicants respectfully request reconsideration of the rejection of claim 19 as being unpatentable over the proposed combination of Ellis in view of Yoon and Woodhill for at least the reasons discussed above with respect to claim 16.

VI. CONCLUSION

For at least the reasons discussed above, the Applicants respectfully submit that the pending claims are allowable in all respects. Therefore, the Board is respectfully requested to reverse the rejections of pending claims 1-26.

VII. PAYMENT OF FEES

The Commissioner is authorized to charge any necessary fees, including the $540 fee for this Appeal Brief, the $540 fee for the Notice of Appeal and any other necessary fees, or credit overpayment to Deposit Account 13-0017.

Respectfully submitted,

Dated: May 27, 2009

/Joseph M. Butscher/
Joseph M. Butscher
Registration No. 48,326

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
(312) 775-8000
(312) 775-8100 (fax)

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1. A method for establishing a communication pathway for subsequent media exchanges between a television display in a first home and storage that contains media in a second home, the method comprising:

securely receiving address correlation information associated with the television display in the first home;

securely receiving address correlation information associated with the storage in the second home;

requesting affirmative confirmation using said received address correlation information associated with one or both of the television display and/or the storage; and

storing said affirmative confirmation.

2. The method according to claim 1, comprising associated with the subsequent media exchanges, verifying that said affirmative confirmation has been stored.

3. The method according to claim 2, comprising receiving one or both of said address correlation information associated with the television display in the first home and/or said address correlation information associated with the storage in the second home via one or both of an in-band channel and/or an out-of-band channel.

4. The method according to claim 1, wherein one or both of said address correlation information associated with the television display in the first home and/or said address correlation information associated with the storage in the second home is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification and/or a key.

5. The method according to claim 1, comprising limiting a period for which one or both of said address correlation information associated with the television display in the first home and/or said address correlation information associated with the storage in the second home is valid.

6. A method for establishing a communication pathway for subsequent media exchange between a first media component in a first home and a second media component in a second home, the method comprising:

receiving at least one of address correlation information associated with the first media component in the first home and a routing address associated with the first media component in the first home;

receiving address correlation information associated with the second media component in the second home; and

requesting confirmation using the address correlation information associated with the second media component.

7. The method according to claim 6, comprising storing said confirmation.

8. The method according to claim 7, comprising associated with the subsequent media exchange, verifying that said confirmation has been stored.

9. The method according to claim 6, comprising receiving one or more of said address correlation information in said first home, said address correlation information in said second home and/or said routing address via one or both of an in-band channel and/or an out-of-band channel.

10. The method according to claim 6, wherein one or both of said address correlation information in said first home and/or said address correlation information in

said second home is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification and/or a key.

11. The method according to claim 6, comprising limiting a period for which one or both of said address correlation information in said first home and/or said address correlation information in said second home is valid.

12. A system that supports media exchange between a first home and a second home, the system comprising:

a television display in the first home, said television display having an associated first routing address;

storage that contains media in a second home, said storage having an associated second routing address; and

a server component that establishes a secure communication pathway through which media contained in the second home is delivered to said television display in the first home, wherein one or more of said television display, said storage and/or said server requests affirmative confirmation using one or both of said first and/or second associated routing addresses.

13. The system according to claim 12, wherein said server comprises a memory that stores one or both of said first routing address and/or said second routing address.

14. The system according to claim 12, wherein said one or both of said first routing address and/or said second routing address is communicated via one or both of an in-band channel and/or an out-of-band channel.

15. The system according to claim 12, wherein said server authenticates an initial access of one or both of said television display having an associated first routing address and/or said storage having an associated second routing address.

16. A system for communicating information, the system comprising:

at least one processor that issues access information from a first device to at least a second device;

said at least one processor transfers at least a portion of said access information to a third device; and

said at least one processor authenticates said access information by said first device when said third device attempts to transfer at least one of media data and service to said at least said second device.

17. The system according to claim 16, wherein said at least one processor communicates said access information from said at least said second device to said third device.

18. The system according to claim 17, wherein said at least one processor communicates said access information from said at least said second device to said third device via one or both of an in-band channel and/or an out-of-band channel.

19. The system according to claim 17, comprising a telephone device that is utilized to inform a user of said third device of said access information.

20. The system according to claim 16, wherein said first device is a media exchange server.

21. The system according to claim 16, wherein said at least said second device and said third device is one or more of a media processing system, a personal computer executing media exchange software and/or a media peripheral.

22. The system according to claim 16, wherein said at least one processor permits said third device to communicate with said at least said second device, if said access information is authenticated by said first device.

23. The system according to claim 16, wherein said at least one processor one or both of denies and/or restricts said transfer of said at least one of media data and service between said at least said second device, if said access information is not authenticated by said first device.

24. The system according to claim 16, wherein said access information is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification and/or a key.

25. The system according to claim 16, wherein said at least one processor limits a period for which said access information is valid.

26. The system according to claim 16, wherein said at least one processor is one or more of a computer processor, a media peripheral processor, a media exchange system processor, a media exchange server processor and/or a media processing system processor.

EVIDENCE APPENDIX
(37 C.F.R. § 41.37(c)(1)(ix))

(1) U.S. 6,774,926 ("Ellis"), entered into record by Examiner in August 26, 2008 Office Action.

(2) U.S. 2003/0177249 ("Takanashi"), entered into record by Examiner in August 26, 2008 Office Action.

(3) U.S. 6,182,094 ("Humpleman"), entered into record by Examiner in August 26, 2008 Office Action.

(4) U.S. 2002/0004832 ("Yoon"), entered into record by Examiner in August 26, 2008 Office Action.

(5) U.S. 6,934,858 ("Woodhill"), entered into record by Examiner in August 26, 2008 Office Action.

RELATED PROCEEDINGS APPENDIX
(37 C.F.R. § 41.37(c)(1)(x))

Not applicable.